IFV Instituut Fysieke Veiligheid

Kennis en kunde voor regionale cybergevolgbestrijding

Instituut Fysieke Veiligheid
Kennisontwikkeling en onderwijs
Postbus 7010
6801 HA Arnhem
Kemperbergerweg 783, Arnhem
www.ifv.nl
info@ifv.nl
026 355 24 00

Colofon

Instituut Fysieke Veiligheid (2021). *Kennis en kunde voor regionale cybergevolgbestrijding.* Arnhem: IFV.

Opdrachtgever:	Portefeuillehouder Cyber en digitale ontwrichting
Contactpersoon:	Sjoerd Hooymans- Secretaris werkgroep Cyber en digitale ontwrichting
Titel:	Kennis en kunde voor regionale cybergevolgbestrijding
Datum:	28 december 2021
Auteurs:	Laurens van der Varst, Jana Domrose, Mees Janssen, Ellis Brouwer
Projectleider:	Laurens van der Varst
Review:	Menno van Duin
Eindverantwoordelijk:	Menno van Duin

Samenvatting

In opdracht van de portefeuillehouder Digitale Ontwrichting en Cyber heeft het lectoraat Crisisbeheersing (IFV) een verkenning gedaan naar de benodigde kennis en kunde voor regionale cybergevolgbestrijding. Om in beeld te kunnen brengen welke kennis en kunde veiligheidsregio's nodig hebben voor de gevolgbestrijding van cyberincidenten en hoe deze kennis en kunde kan worden gemobiliseerd, zijn de volgende onderzoeksvragen geformuleerd:

1. Welke kennis en kunde zijn beschikbaar in veiligheidsregio's voor de (voorbereiding op de) bestrijding van cyberincidenten?
2. Welke kennis en kunde ontbreken nog binnen veiligheidsregio's voor de (voorbereiding op de) bestrijding van cyberincidenten?
3. Welke lessen over kennis en kunde komen voort uit geëvalueerde incidenten en oefeningen binnen veiligheidsregio's?
4. Hoe kunnen veiligheidsregio's benodigde cyberkennis en -kunde voor de bestrijding van cyberincidenten mobiliseren?

Uit het onderzoek blijkt dat kennis en kunde voor cybergevolgbestrijding in veiligheidsregio's beperkt aanwezig is. Voor veiligheidsregio's is het lastig meer ervaring en expertise op te bouwen op dit nieuwe crisisdomein, doordat het aantal cyberverstoringen waarbij de inzet van regio's nodig is (tot op heden) beperkt is. De vraag welke expertise nodig is hangt bovendien samen met de omvang, ernst en complexiteit van de verstoring die zich voordoet. De in dit onderzoek geïnventariseerde cyberkennis en -kunde vormt een startpunt voor nader onderzoek, dialoog en opbouw van een body of knowledge.

Uit diverse studies blijkt dat meerdere kennisdisciplines (ICT, cybersecurity expertise, crisisbeheersing, bedrijfsvoering) nodig zijn voor de respons op cyberincidenten én dat die disciplines onderling te weinig verbonden zijn. Aangrijpingspunten om de verschillende disciplines beter met elkaar te verbinden zijn:

> Verhogen van het kennispeil over cyber onder crisisfunctionarissen zoals operationeel leiders, communicatieadviseurs en bedrijfsvoering is nodig, door bijvoorbeeld bijscholing, het uitwisselen van ervaringen met collega's, kennisnemen en doorleven van planvorming en oefenen. Dat is relevant voor de bestrijding van interne en externe cyberincidenten. Bijscholing zou in elk geval de onderwerpen uit tabel 4.2 betreffen, waaronder van de partners die over kennis beschikken bij een cybercrisis.
> Verhogen van het kennispeil van crisisbeheersing onder ICT-functionarissen door bijvoorbeeld bijscholing, meedoen met crisisoefeningen, kennisnemen en doorleven van planvorming. Dat is relevant voor de bestrijding van interne cyberincidenten.
> Het is nodig om binnen de organisatie te investeren in bruggenbouwers/liaisons die verschillende kennisdisciplines met elkaar kunnen verbinden. Denk aan een tactisch-strategisch ingestelde 'OvD-Cyber' of adviseur Cyber. Zie voor de benodigde kennis en kunde van zo'n functionaris tabel 4.2.
> Gezamenlijke scenario-/oefenbijeenkomsten zijn onontbeerlijk, waarin verschillende disciplines in gesprek gaan over de bijdrage die zij kunnen leveren aan de incidentrespons.

Inhoud

Inleiding

Aanleiding

De kwetsbaarheden en dreigingen in het digitale domein nemen gestaag toe (NCTV, 2018). Dreigingen als sabotage, informatiemanipulatie, informatiediefstal, spionage, storingen of lekken liggen tegenwoordig constant op de loer (NCTV, 2020). Uit casussen zoals de cyberaanval op de Rotterdamse haven (2017), de uitval van 112 door de KPN-storing (2019) en kwetsbaarheden in de Citrix-software (2020) blijkt dat grootschalige cyberincidenten met eventuele maatschappelijke gevolgen realistisch zijn. Daarnaast nemen ook de kwetsbaarheden in het digitale domein toe. Zo raken de fysieke en digitale wereld door de toename van digitale ontwikkelingen en mogelijkheden steeds meer met elkaar vervlochten (NCTV, 2018). De toename van menselijke afhankelijkheid van digitale processen kan bij een cyberincident leiden tot directe schade aan de economie of nationale veiligheid (NCTV, z.d.). Hierbij kan onder andere worden gedacht aan een uitval van vitale infrastructuur zoals de elektriciteits- of drinkwatervoorziening, het internet of betalingsverkeer. De dreiging neemt derhalve toe: maatschappelijke processen kunnen door de digitale ontwikkelingen makkelijker op grote schaal worden verstoord.

Om deze reden is het voorbereiden en reageren op cyberincidenten een actueel thema binnen veiligheidsregio's. In 2020 heeft het lectoraat Crisisbeheersing van het Instituut Fysieke Veiligheid een onderzoek naar veiligheidsregio's en cyberrisico's uitgevoerd (IFV, 2020). Eén van de vraagstukken die naar aanleiding van dit onderzoek speelt, is welke kennis en kunde nodig zijn binnen de veiligheidsregio's om voorbereid te zijn op interne en externe cyberincidenten. Daarom heeft de portefeuillehouder Digitale Ontwrichting en Cyber het lectoraat Crisisbeheersing gevraagd een verkenning uit te voeren naar de benodigde kennis en kunde voor regionale cybergevolgbestrijding in een vervolgonderzoek. Doelstelling is om in kaart te brengen over welke kennis en kunde veiligheidsregio's reeds beschikken voor de gevolgbestrijding van cyberincidenten en welke cyberkennis en -kunde juist nog gemobiliseerd dienen te worden.

Vraagstelling

Om in beeld te kunnen brengen welke kennis en kunde veiligheidsregio's nodig hebben voor de gevolgbestrijding van cyberincidenten en welke mogelijkheden voor de mobilisering van deze kennis en kunde voor de regionale crisisbeheersing bestaan, zijn de volgende onderzoeksvragen geformuleerd:

1. Welke kennis en kunde zijn beschikbaar in veiligheidsregio's voor de (voorbereiding op de) bestrijding van cyberincidenten?
2. Welke kennis en kunde ontbreken nog binnen veiligheidsregio's voor de (voorbereiding op de) bestrijding van cyberincidenten?
3. Welke lessen over kennis en kunde komen voort uit geëvalueerde incidenten en oefeningen binnen veiligheidsregio's?

4. Hoe kunnen veiligheidsregio's benodigde cyberkennis en -kunde voor de bestrijding van cyberincidenten mobiliseren?

Aanpak

Om de onderzoekvragen te beantwoorden zijn op drie manieren gegevens verzameld, namelijk via een documentstudie, een uitvraag onder medewerkers van veiligheidsregio's (zowel middels interviews als een enquête) en interviews met deskundigen en vitale partners. Deze methoden worden hieronder nader toegelicht.

Documentstudie en interviews

Voor het deelonderzoek naar de benodigde kennis en kunde over regionale cyberrisico's en -dreigingen en het deelonderzoek naar de benodigde kennis en kunde voor de planvorming en cyberrespons, zijn bestaande documenten zoals de *Handreiking Cybergevolgbestrijding* (Berenschot, 2020), *Whitepaper digitale ontwrichting en cyber* (IFV, 2019) en het adviesrapport *Voorbereiden op digitale ontwrichting* (WRR, 2019) geraadpleegd. Daarnaast is dergelijke benodigde kennis en kunde middels de interviews en enquête uitgevraagd en aangevuld. Tevens zijn achtergrondgesprekken gevoerd met deskundigen en medewerkers van vitale partners.

Uitvraag onder veiligheidsregio's

De uitvraag onder veiligheidsregio's heeft langs twee lijnen plaatsgevonden. In de beginfase van het onderzoek is een aantal interviews afgenomen met personen die werkzaam zijn binnen een veiligheidsregio of binnen hun functie partner zijn van een veiligheidsregio, waardoor zij kennis hebben van de crisisstructuur binnen veiligheidsregio's en/of de gevolgbestrijding van cyberincidenten. Deze interviews hadden een oriënterende functie en gaven meer inzicht in de benodigde kennis en kunde over cyberrisico's en -dreigingen, de planvorming en cyberrespons en de mate waarin, volgens de respondenten, deze kennis en kunde aanwezig zijn binnen de veiligheidsregio's. De interviews vonden plaats tussen 22 februari en 8 april 2021.

Om daarnaast op grotere schaal in kaart te brengen welke kennis en kunde binnen veiligheidsregio's nodig zijn voor de gevolgbestrijding van cyberincidenten, is een online enquête uitgezet onder leden van de Werkgroep Digitale Ontwrichting en Cyber en het VR-ISAC. Ook is middels deze enquête de manier onderzocht waarop veiligheidsregio's momenteel cyberkennis en -kunde voor de gevolgbestrijding van cyberincidenten mobiliseren en is bekeken welke behoeften er binnen veiligheidsregio's zijn voor het mobiliseren van ontbrekende kennis en kunde. De uitvraag liep van 29 maart tot 16 april 2021. In totaal hebben 38 respondenten de enquête ingevuld (21 van de werkgroep en 17 van het VR-ISAC). Na afloop van de deadline zijn de data van de interviews en enquêtes samengevoegd en zijn er descriptieve analyses uitgevoerd om landelijke totalen in kaart te brengen. De resultaten van het onderzoek zijn toegelicht aan de werkgroep Digitale Ontwrichting en Cyber op 9 december, waarbij geïnventariseerd is welke cyberkennis en -kunde 'mee te geven' aan crisisfunctionarissen.

Leeswijzer

In hoofdstuk 1 wordt de achtergrond van dit onderzoek geschetst; centrale begrippen worden toegelicht en er wordt bekeken wat volgens de evaluatie van de wet Veiligheidsregio de rol is van de veiligheidsregio's bij de bestrijding van cyberincidenten. Hoofdstuk 2 gaat in op de resultaten uit de enquête over benodigde cyberkennis en -kunde in veiligheidsregio's, en in hoofdstuk 3 wordt bekeken welke best practices veiligheidsregio's kunnen meenemen om hun interne cyberweerbaarheid en externe cybergevolgbestrijding te versterken. Het vierde en laatste hoofdstuk bevat de conclusies van dit onderzoek en enkele aanbevelingen.

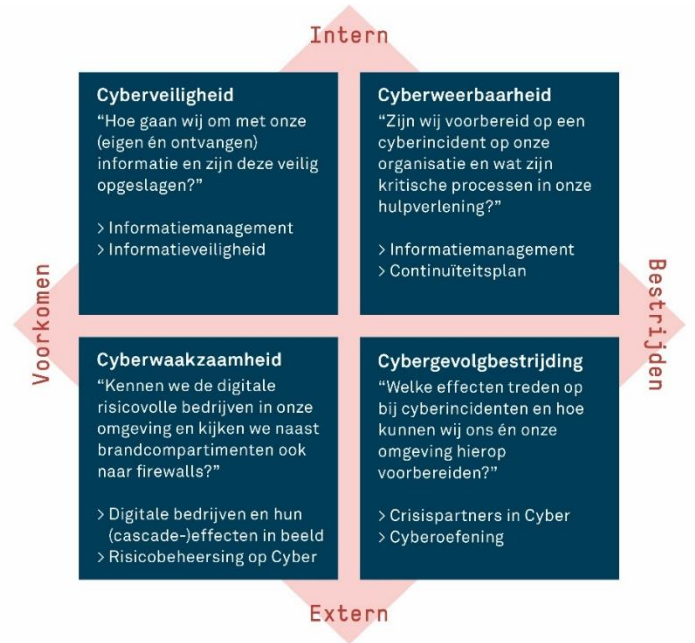
1 Achtergrond

In dit hoofdstuk worden de centrale begrippen uit het onderzoek toegelicht en wordt de focus van het onderzoek nader afgebakend. Ook beschouwen wij wat er uit de recente evaluatie van de wet Veiligheidsregio naar voren komt over de rol van veiligheidsregio's bij de bestrijding van cyberincidenten.

1.1 Wat zijn cyberweerbaarheid en -gevolgbestrijding?

In dit onderzoek is aangesloten bij de begrippen zoals gehanteerd door de NCTV in het *Cybersecuritybeeld Nederland* en door het IFV in de *Whitepaper Digitale ontwrichting en cyber* (IFV, 2019). In het *Cybersecuritybeeld Nederland* wordt een cyberincident gedefinieerd als: "Een gebeurtenis of activiteit die de beschikbaarheid, integriteit of vertrouwelijkheid van informatie- en procesbesturingssystemen aantast" (NCTV, 2020). Hierbij kan bijvoorbeeld worden gedacht aan een hack die het betalingsverkeer platlegt of een aanval die processen, bestanden of systemen van een vitale organisatie versleutelt.

In de *Whitepaper Digitale ontwrichting en cyber* wordt met betrekking tot digitale weerbaarheid van veiligheidsregio's gerefereerd aan een cyberkwadrant, dat in 2018 werd opgesteld door Veiligheidsregio IJsselland. In het kwadrant (zie figuur 1.1) worden vier componenten binnen het domein van 'cyber' onderscheiden, namelijk:
1. cyberveiligheid
2. cyberweerbaarheid
3. cyberwaakzaamheid
4. cybergevolgbestrijding.



Figuur 1.1 Het cyberkwadrant zoals uitgewerkt door Veiligheidsregio IJsselland

De centrale focus in dit onderzoek ligt op de bestrijdende component van het kwadrant, zowel wat betreft interne (cyberweerbaarheid) als externe cyberincidenten (cybergevolgbestrijding). Het betreft dus alle handelingen die erop gericht zijn de gevolgen te verminderen van een cyberincident. Deze handelingen zijn bijvoorbeeld noodzakelijk wanneer een cyberaanval processen, bestanden of systemen van de organisatie versleutelt of wanneer er door een technische storing bepaalde systemen niet kunnen worden gebruikt. Cybergevolgbestrijding behelst alle activiteiten in het kader van het beperken van de effecten van een cyberincident, waarvan de oorzaak en/of de gevolgen in het werkgebied van de veiligheidsregio ligt. Denk hierbij aan de reactie op een verstoring van vitale infrastructuur binnen de regio.

1.2 Wat zijn cyberkennis en -kunde?

In dit onderzoek beschouwen wij welke kennis en kunde nodig zijn voor cybergevolgbestrijding in veiligheidsregio's. Weggeman (2007) ziet kennis als het vermogen om een bepaalde taak te verrichten, waarbij een combinatie van informatie, ervaring, vaardigheden en houding een rol spelen. Daarbij maakt Romiszowski (1981) een onderscheid tussen reproductieve en productieve vaardigheden. Reproductieve vaardigheden zijn het vermogen om eenvoudige acties en standaardprocedures toe te passen; bij productieve vaardigheden gaat om geleerde vaardigheden in nieuwe situaties kunnen gebruiken. Hiermee wordt de ontwikkeling van kennis en kunde zichtbaar. Naarmate beroepsbeoefenaren naast feitelijke kennis steeds meer beschikken over een bredere begripsvorming en kennis actief gaan toepassen in de praktijk, groeit hun vakbekwaamheid. Het gaat dus om méér dan het *hebben* van feitelijke kennis, maar juist ook om bredere begripsvorming en het *toepassen* van kennis in verschillende praktijksituaties. Het kunnen toepassen van kennis scharen we in dit onderzoek onder kunde: vaardigheden en houding. In tabel 1.2 zijn de belangrijkste kenmerken van kennis en kunde nogmaals samengevat.

Tabel 1.2 Kenmerken van kennis en kunde

Wat	Beschrijving
Kennis	Beschikken over feitelijke informatie, waaronder bevoegdheden en verantwoordelijkheden, actoren, plannen, protocollen, handreikingen en draaiboeken.
Kunde (vaardigheden en houding)	Toepassen van kennis in verschillende situaties met behulp van specifieke vaardigheden (zoals luisteren, analyseren en structuren) en houding (zoals open, nieuwsgierig en daadkrachtig).

1.3 Aandachtspunten uit de evaluatie wet Veiligheidsregio's

Na het afbakenen van het theoretische kader rondom kennis en kunde over cyberweerbaarheid en cybergevolgbestrijding, beschouwen we welke rol en taken veiligheidsregio's officieel hebben bij digitale verstoringen. Aangezien het bestrijden van interne cyberincidenten vooral in het belang van de eigen organisatie is, richten wij ons in deze beschouwing op de verantwoordelijkheden van de veiligheidsregio met betrekking tot cyberincidenten in haar verzorgingsgebied.

Volgens art. 10 Wet veiligheidsregio's zijn de veiligheidsregio's verantwoordelijk voor het voorkomen en bestrijden van branden, het voorbereiden op risico's, rampen en crises en de coördinatie, beheersing en bestrijding van rampen en crises. Volgens dit artikel zijn veiligheidsregio's alleen verantwoordelijk voor de effectbestrijding van een cyberincident wanneer dit incident leidt tot een (ernstige) bedreiging voor de fysieke veiligheid en/of tot maatschappelijke ontwrichting. Kortom: veiligheidsregio's zijn bij een extern cyberincident alleen aan zet voor de bestrijding van de fysieke en/of maatschappelijke gevolgen daarvan.

In 2020 heeft de evaluatiecommissie Wet veiligheidsregio's in opdracht van de minister van Justitie en Veiligheid onderzocht in hoeverre de huidige Wet veiligheidsregio's bijdraagt aan de beheersing van risico's voor burgers en de aanpak van incidenten en crises, en hoe de wet aansluit op actuele trends in crises, de crisisbeheersing en brandweerzorg. Met het oog op het stijgende aantal risico's rondom digitale verstoringen stelt de evaluatiecommissie (2020) dat veiligheidsregio's hun rol als partij in een cybercrisis nog moeten vinden. Er wordt door samenwerkingspartners en de samenleving veel van veiligheidsregio's verwacht, maar het is bijna onmogelijk om hier met de huidige kennis, vaardigheden, en bevoegdheden aan te voldoen. De veiligheidsregio's moeten volgens de evaluatiecommissie daarom vooral zorgen voor een effectief cybernetwerk (met onder andere Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) en Nationaal Cyber Security Centrum (NCSC)) en dienen binnen dit netwerk op te treden als coördinerende partij.

Hieruit wordt duidelijk dat veiligheidsregio's vooral moeten investeren in relaties en netwerken met andere partijen. Ze zullen niet over alle expertise zelf te hoeven beschikken, maar het is wel handig te weten waar expertise vandaan te halen (zie ook: IFV, 2021). Dat vraagt van regio's wel enig begrip van het cyberspeelveld en zelfkennis: kennis over de eigen rol en verantwoordelijkheid in een cybernetwerk én kennis over het eigen 'cybervermogen'. Dat laatste wil zeggen: welke expertise de veiligheidsregio zelf in huis heeft voor incidentrespons en herstel en voor welke deskundigheid en skills cybersecurity-experts nodig zijn.

2 Cyberkennis en -kunde in veiligheidsregio's

In dit hoofdstuk beschrijven we de resultaten uit de enquête over benodigde cyberkennis en -kunde in veiligheidsregio's. Hoewel er per veiligheidsregio slechts maximaal twee respondenten bevraagd zijn over cyberweerbaarheid en cybergevolgbestrijding[1], refereren wij in de navolgende paragrafen omwille van de leesbaarheid aan 'de veiligheidsregio's'.

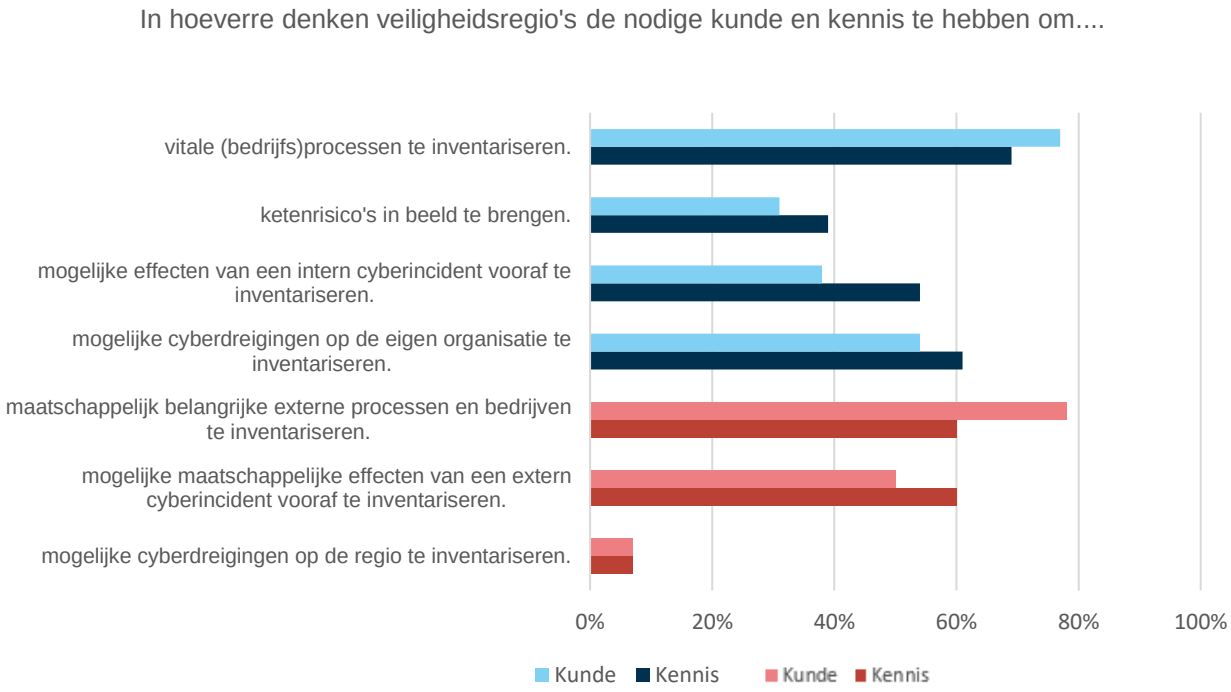
2.1 Soorten kennis en kunde

2.1.1 Kennis en kunde nodig voor de voorbereiding op cyberincidenten

In de enquête zijn respondenten gevraagd in hoeverre hun organisatie in staat is om zich voor te bereiden op mogelijke interne en externe cyberincidenten, en of ze denken dat de hiervoor benodigde kennis en kunde binnen de eigen organisatie of juist bij externe partners belegd zou moeten worden. Opvallend is dat veiligheidsregio's zowel qua kennis (58%) als kunde (50%) duidelijk beter in staat blijken te zijn om cyberdreigingen voor de eigen organisatie in beeld te brengen dan dreigingen voor de gehele regio. Twee derde van de bevraagde veiligheidsregio's denkt dan ook dat kennis en kunde voor de inventarisatie van *interne* dreigingen vooral intern belegd moeten worden, terwijl slechts een derde van de bevraagden denkt dat de inventarisatie van *externe* dreigingen opgave is van de veiligheidsregio. De nodige kennis en kunde zouden regio's liever bij externe bedrijven willen beleggen.

Ook is aan de regio's gevraagd of zij voldoende kennis en kunde in huis hebben om de gevolgen van interne en externe cyberincidenten te inventariseren. Uit de resultaten blijkt dat ruim de helft van de bevraagde regio's voldoende kennis denkt te hebben, en een derde voldoende kunde om de mogelijke effecten van een intern cyberincident in beeld te brengen. De eventuele maatschappelijke effecten van een cyberincident binnen het werkgebied van de regio weet zelfs (iets meer dan) de helft van de bevraagde regio's in kaart te brengen. Rond 60% heeft hiervoor de nodige kennis en 50% de nodige kunde. Respondenten zijn het er dan ook over eens dat veiligheidsregio's zelf de nodige kennis en kunde in huis dienen te hebben om in de koude fase een effectanalyse voor interne en externe cyberincidenten door te voeren.

[1] Uiteraard kunnen we niet garanderend dat de antwoorden van de respondent representatief zijn voor de opvattingen die dominant zijn binnen zijn of haar veiligheidsregio. De rol of functie van de geselecteerde respondenten laat ons echter aannemen dat zij voldoende zicht hebben op de vragen en thema's die er in de regio spelen op het gebied van cyber.



Figuur 2.1. Mate waarin veiligheidsregio's denken de nodige kunde en kennis in huis te hebben om risico's en effecten van interne (blauw) en externe (rood) cyberincidenten in beeld te brengen.

Op de vraag wat regio's nodig hebben voor de voorbereiding op interne en externe cyberincidenten, geven meerdere respondenten aan dat er binnen de organisatie meer sprake zou moeten zijn van bewustwording, auditing en lerend vermogen met betrekking tot interne cyberincidenten. Het blijkt voor regio's hierbij een uitdaging om ingewikkelde onderwerpen rondom cyber toegankelijk te maken voor functionarissen. Wat betreft de voorbereiding op externe cyberincidenten geven respondenten aan een netwerk nodig te hebben met relevante partners, evenals duidelijkheid rondom taken en verantwoordelijkheden bij een digitale verstoring. Regio's ervaren het met name als lastig om relevante externe bedrijven (anders dan vitale partners) in kaart te brengen en aan te haken bij hun cyberkennis en -kunde. Ook zou men binnen de regio's meer zicht willen hebben op mogelijk domino- of cascade-effecten bij cyberstoringen in externe bedrijven binnen het verzorgingsgebied van de regio. Hiervoor is er volgens de respondenten een tekort aan technische kennis bij de functionarissen van de regionale crisisorganisatie.

2.1.2 Kennis en kunde nodig voor het inschatten van oorzaak, duur en impact van een verstoring

Uit de uitvraag blijkt dat veiligheidsregio's naar eigen zeggen beter de oorzaak kunnen inschatten van een *intern* dan van een *extern* cyberincident. Het percentage respondenten dat denkt voldoende kennis en kunde te hebben om *interne* en *externe* oorzaken van cyberincidenten in beeld te brengen, is met respectievelijk 25% en 15% echter vrij laag.

Tevens is aan respondenten gevraagd in hoeverre zij denken de duur van een cyberincident in te kunnen schatten. Slechts 10% van de bevraagden heeft naar eigen zeggen voldoende kennis en kunde om deze voor *interne* cyberincidenten te voorspellen. Wat betreft *externe* incidenten geeft het merendeel van de respondenten aan dat het *niet* beschikt over de

nodige kennis (92%) en kunde (66%) om de duur van de verstoring in te schatten. De overige respondenten hebben hier geen duidelijke mening over.

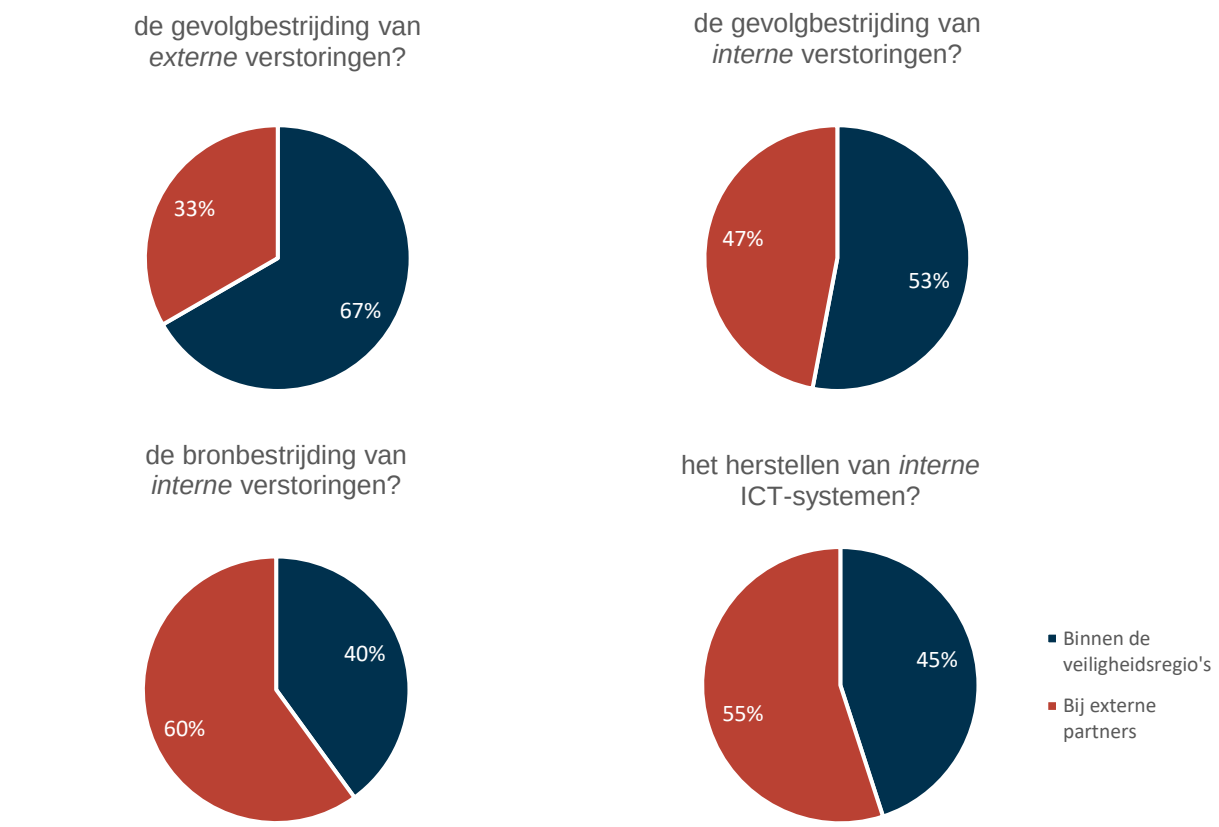
Wat betreft het kunnen inschatten van de impact van een *extern* cyberincident op maatschappelijke processen zijn respondenten daarentegen optimistischer. De helft denkt dat zijn regio hiervoor voldoende kennis in huis heeft en iets meer dan de helft (57%) denkt dat de regio tevens over voldoende kunde beschikt. Ook voor het inschatten van de impact van een *intern* cyberincident op organisatieprocessen heeft de meerderheid van de bevraagde regio's naar eigen zeggen voldoende kennis (69%) en kunde (58%). Meer dan twee derde (67%) van de respondenten geeft tevens aan dat er binnen de organisatie voldoende kennis is om geraakte interne systemen te kunnen identificeren; de helft weet de schade aan ICT-systemen te identificeren.

De meerderheid van de respondenten vindt dat de kennis voor het inschatten van oorzaak, duur en impact van een *extern* incident bij externe partijen zou moeten worden belegd. Over de vraag of dit ook voor *interne* cyberincidenten geldt, zijn de meningen verdeelt. De helft van de bevraagden vindt dat veiligheidsregio's deze kennis en kunde zelf in huis dienen te hebben.

2.1.3 Kennis en kunde nodig voor het beperken van de effecten van een verstoring

De laatste vragen over (benodigde) cyberkennis en -kunde in veiligheidsregio's hebben betrekking op het kunnen verminderen of bestrijden van de gevolgen van een cyberincident. Bijna twee derde (64%) van de respondenten geeft aan dat de eigen organisatie zowel voldoende kennis als kunde in huis heeft om de effecten van een *extern* cyberincident te bestrijden. De overige respondenten hebben hier geen duidelijke mening over. Wat betreft het bestrijden van *interne* cyberincidenten zijn veiligheidsregio's minder optimistisch. Slechts een derde van de bevraagden denkt dat de eigen regio voldoende kennis in huis heeft om de gevolgen van een interne verstoring te verkleinen, 17% denkt dat er hiervoor sprake is van voldoende kunde. Zo'n 42% van de respondenten denkt dat er voldoende kennis in huis is om schade aan eigen ICT-systemen te herstellen. Aan de andere kant geeft 82% aan dat de veiligheidsregio waarschijnlijk *niet* de bron van de *interne* verstoring kan bestrijden.

Twee derde van de bevraagden vindt dat veiligheidsregio's qua kennis en kunde zelf in staat moeten zijn om de gevolgen van een *extern* cyberincident te bestrijden. Over de juiste plek voor kennis en kunde voor de gevolgbestrijding van *interne* verstoringen zijn veiligheidsregio's wederom verdeeld. 53% geeft aan dat veiligheidsregio de kennis daarvoor zélf in huis moet hebben, terwijl 47% denkt dat die kennis bij externe partijen zou moeten worden belegd (zie ook figuur 2.2). Wat betreft de bronbestrijding van interne cyberincidenten en het herstellen van de ICT-systemen zijn respondenten daarentegen iets meer geneigd om de nodige kennis extern te beleggen (respectievelijk 60% en 55%).



Figuur 2.2 Partijen waar specifieke cyberkennis en -kunde volgens veiligheidsregio's moet worden geborgd.

2.1.4 Waar ligt relevante kennis en kunde?

Tot slot werden veiligheidsregio's gevraagd welke specifieke interne functionarissen en externe partners volgens hen een rol spelen bij het borgen van kennis en kunde over interne en externe cyberincidenten.

Interne expertise

Wat betreft kennis en kunde over *interne* cyberincidenten zijn volgens de respondenten met name ICT-medewerkers belangrijke spelers. 36% van de respondenten denkt dat (onder anderen) zij kennis en kunde in huis moeten hebben over de bestrijding van interne verstoringen.[2] Daarnaast denkt 32% van de respondenten dat de kennis bij een CISO (Chief Information Security Officer) kan worden belegd. 16% ziet (tevens) een rol weggelegd voor medewerkers crisisbeheersing. Enkele respondenten hebben aanvullende ideeën voor het beleggen van de kennis binnen de organisatie. Zo is geopperd dat er kennis zou kunnen liggen bij een "(Technical) Information Security Officer," een toekomstig VR-CERT en de directie.

Voor de gevolgbestrijding van *externe* cyberincidenten zou kennis binnen de eigen organisatie bij medewerkers crisisbeheersing moeten liggen, zo geeft bijna de helft (48%) van de

[2] Noot: respondenten konden bij deze vraag meerdere antwoorden selecteren. De som van de percentages hoeft derhalve geen 100% te zijn.

respondenten aan. Een kwart (24%) van de respondenten zou de kennis binnen de organisatie (ook) bij een CISO willen beleggen en slechts 11% bij ICT-medewerkers.

Benodigde cyberkennis en -kunde voor crisisfunctionarissen (bron: werkgroep Digitale ontwrichting en cyber, 9 december 2021)

Leden van de werkgroep Digitale ontwrichting en cyber geven aan, dat crisisfunctionarissen binnen veiligheidsregio's over de volgende kennis en kunde dienen te beschikken, om voorbereid te zijn op cyberincidenten:

> Kennis van rollen en verantwoordelijkheden van veiligheidsregio's bij cyberincidenten.
> Bestuurlijke uitgangspunten kennen in relatie tot cyber.
> Weten welke cyberspecifieke teams actief zijn.
> Netwerk van crisisorganisaties bij partners kennen (o.a. IBD, Zorg-CERT, NCSC).
> Inzicht in dilemma's bij cyberincidenten.
> Scenariodenken/ incident vertalen naar (maatschappelijke) impact.
> Impact kunnen vertalen voor het bestuur
> Bewustzijn dat je als veiligheidsregio niet iet alles zelf moet doen; gebruik maken van je netwerk.

Externe partners

Voor de kennisborging voor de bestrijding van *externe* cyberincidenten zien respondenten een rol voor meerdere partijen. Organisaties waar kennis vandaan zou kunnen worden gehaald zijn zowel het Nationaal Cyber Security Center (17%), als private kennis-en adviesbureaus zoals Fox-IT (17%), publieke kennisinstellingen (16%), landelijke voorzieningen zoals het Veiligheidsregio Information Sharing and Analysis Center (14%), landelijke netwerken zoals de werkgroep Digitale ontwrichting en cyber (12%) en andere veiligheidsregio's (12%). Het Instituut Fysieke Veiligheid is met 7% relatief weinig genoemd. Aanvullend genoemde organisaties zijn IBD, Digital Trust Center (DTC), getroffen organisatie(s), de politie en betrokken ministeries.

Voor de bestrijding van interne cyberincidenten wordt er bij voorkeur hulp ingewonnen van het Nationaal Cyber Security Center (19%), private kennis- en adviesbureaus (19%) en landelijke voorzieningen zoals het Veiligheidsregio Information Sharing and Analysis Center (19%) of andere veiligheidsregio's (17%). Landelijke netwerken (10%), het Instituut Fysieke Veiligheid (8%) en publieke kennisinstellingen zoals hogescholen en universiteiten (3%) worden minder vaak genoemd. Daarnaast worden de volgende organisaties en informatiebronnen genoemd:

> KPN-Security-CERT, Deloitte-CERT
> vakgroep informatieveiligheid
> het internet in algemene zin
> IBD
> politie (Team digitale opsporing).

2.2 Bewustzijn en middelen in de veiligheidsregio's

Naast kennis en kunde is er in de enquête ook gevraagd naar het bewustzijn binnen veiligheidsregio's wat betreft digitale risico's en naar de middelen die beschikbaar zijn binnen de organisaties om cyberincidenten te bestrijden. De resultaten laten zien dat er bij het management van veiligheidsregio's over het algemeen bewustzijn en belangstelling zijn voor

dit thema, maar dat dit duidelijk meer geldt voor externe (92%) dan interne (50%) dreigingen. Bij operationele functionarissen is daarentegen gemiddeld juist iets meer aandacht voor interne (66%) dan externe (58%) dreigingen binnen het digitale domein.

Ongeveer de helft van de regio's geeft verder aan voldoende technische middelen en systemen in huis te hebben voor de voorbereiding op *externe* cyberincidenten. Voor *interne* cyberincidenten is dit percentage met circa 32% duidelijk lager. Over de beschikbaarheid van financiële middelen, tijd en personeel voor de voorbereiding op externe incidenten is men in de regio's minder goed te spreken. Respectievelijk 85%, 79% en 78% van de bevraagden geeft aan dat deze randvoorwaarden slechts beperkt of helemaal niet beschikbaar zijn voor de voorbereiding op *externe* cyberincidenten. Wat betreft *interne* cyberincidenten geeft maar liefst 100% van de bevraagden aan dat er *niet* voldoende tijd wordt gereserveerd binnen de regio's om voorbereidingen te treffen voor digitale verstoringen. Ook geeft 90% dat er niet voldoende personeel is en 61% dat er *niet* voldoende financiële middelen worden gereserveerd.

2.3 Samenwerken en netwerken met partners

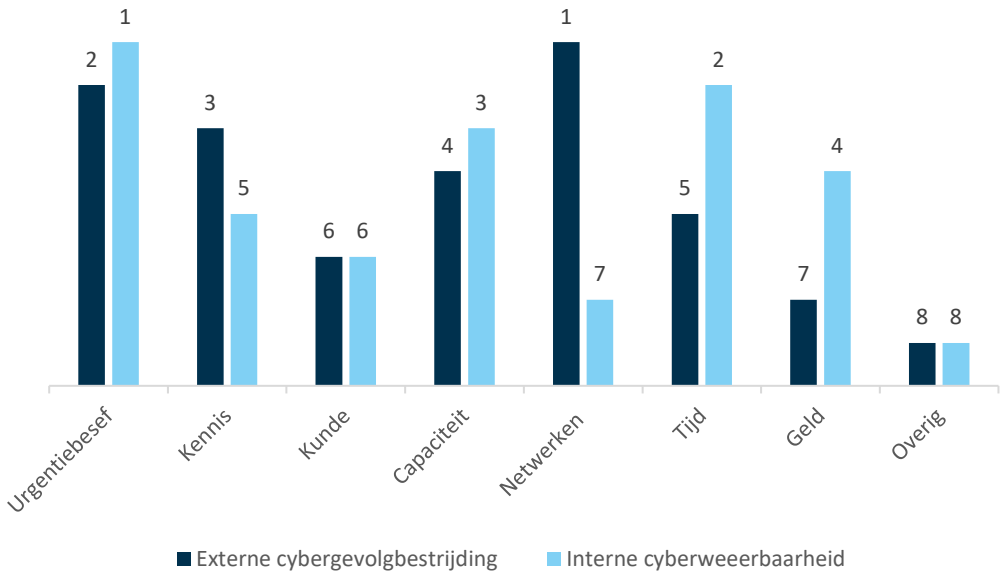
Een ander thema dat uitgevraagd is in de enquête, is samenwerken en netwerken op het gebied van cyber. Uit de resultaten blijkt dat bijna driekwart van de bevraagde veiligheids-regio's zicht lijkt te hebben op overheidsorganisaties en private partijen (zoals het NCSC en private IT-dienstverleners), die hen kunnen helpen bij de voorbereiding op externe cyberincidenten. Met betrekking tot partners voor interne incidenten is dit percentage met 92% zelfs nog hoger. Ook voelt zich respectievelijk 75% en 58% van de regio's (theoretisch) in staat om tijdens de externe en interne cybergevolgbestrijding expertise van samenwer-kingspartners te raadplegen. Wat minder duidelijkheid bestaat er over de verantwoordelijk-heden van de regio en haar partners in het geval van een extern cyberincident. Binnen de helft van de bevraagde regio's heersen hier vragen over.

Wat betreft het thema samenwerken merken respondenten op dat men een cyberincident een keer moet hebben meegemaakt, om te kunnen weten hoe goed en nuttig het netwerk is met partners. Ook blijkt dat er vertrouwen is in de vaardigheden van de operationele functionarissen om in het geval van een verstoring de juiste externe expertise te vinden. Anderen geven aan zich zorgen te maken over het contact tussen Rijk en regio tijdens een digitale verstoring.

2.4 Voorbereiding op cyberincidenten: waar moet de focus liggen?

Veiligheidsregio's geven aan dat er voornamelijk meer aandacht moet zijn voor netwerken en samenwerken om de voorbereiding op *externe* cyberincidenten te kunnen versterken (zie ook figuur 2.3). Ook urgentiebesef is een belangrijk aandachtspunt binnen de regio's. Dat het verhogen van cyberkennis en -kunde binnen de regio's als minder belangrijk wordt gezien, sluit aan bij de eerdere observatie dat men deze bij voorkeur bij externe partijen zou willen beleggen. Ook financiële middelen en tijd zijn dan minder belangrijk.

Wat betreft het versterken van interne cyberweerbaarheid moet de focus volgens respondenten vooral liggen op het verhogen van het urgentiebesef, gevolgd door tijd en capaciteit. Geld, kennis, kunde en netwerken lijken voor regio's actueel minder belangrijke aandachtspunten te zijn voor het versterken van hun cyberweerbaarheid.



Figuur 2.3 Rating van aandachtspunten voor de verbetering van cybergevolgbestrijding en -weerbaarheid in veiligheidsregio's (1 = hoog, 8 = laag).

3 Best practices

In dit hoofdstuk beschouwen wij welke best practices veiligheidsregio's kunnen meenemen om hun interne cyberweerbaarheid en externe cybergevolgbestrijding te versterken. Hierbij kijken we enerzijds wat internationaal als fundamentele cyberkennis en -kunde wordt beschouwd en welke lessen te trekken zijn uit onderzoek naar cyberincidenten in het verleden. Ook vatten wij de belangrijkste lessen samen van de landelijke cyberoefening ISIDOOR-3, die in juni 2021 plaatsvond. Tot slot beschouwen wij hoe vitale partners omgaan met dreigingen uit het digitale domein en wat veiligheidsregio's hiervan kunnen leren.

3.1 Cyber Security Body of Knowledge

In het Verenigd Koninkrijk is een zogeheten 'body of knowledge' voor cybersecurity opgesteld (CyBOK, 2019).[3] Aanleiding was het besef dat kennis over cybersecurity een steeds belangrijker onderdeel wordt van opleidingscurricula, hoewel de essentiële basiskennis in dit vakgebied erg versnipperd is. De 'Cyber Security Body of Knowledge' richtte zich op het bijeenbrengen van algemeen erkende inzichten en kennis op het vlak van cybersecurity. Het zwaartepunt ligt op veiligheid van informatie en systemen en op incidentmanagement. Dit heeft geresulteerd in 21 kennisgebieden (zie tabel 3.1). Elk kennisgebied bevat een beschrijving van erkende begrippen, doelen en benaderingen, inclusief de onderliggende kennisbasis.

De body of knowledge biedt een overzicht van relevante kennisterreinen. Daarnaast toont de body ook de veelzijdigheid van dit veld, waarbinnen verschillende disciplines op het terrein van ICT, security, gedrag en op juridisch vlak samenkomen. Hoewel de kennisgebieden als aparte disciplines worden gepresenteerd, zit er regelmatig overlap tussen. Om veilig systemen te ontwerpen is bijvoorbeeld begrip van menselijk gedrag nodig. Bovendien, zo merken de auteurs op, is enig besef en kennis over aanverwante disciplines handig voor een goed begrip van het grotere geheel en voor onderlinge samenwerking.

Voor veiligheidsregio's kan deze body of knowledge een manier zijn om de eigen kennispositie op het gebied van cybersecurity te inventariseren: welke expertise hebben ze zelf in huis, welke kennis hebben ze nodig, en welke expertise kunnen andere partijen zoals universiteiten, hogescholen of bedrijven leveren?

Tabel 3.1 Cyber Security Body of Knowledge (bron: CyBOK, 2019)

Hoofdthema's	Kennisgebieden
1. Mens, organisatie en regelgeving	1. Risicomanagement en governance 2. Wet- en regelgeving 3. Human factors

[3] Het project is uitgevoerd door experts uit de wereldwijde Cyber Security Community en wordt gefinancierd door het National Cyber Security Program en ondersteund door de UK Cyber Security Raad.

		4. Privacy
2.	Aanvallen en beveiliging	5. Malware en aanvalstactieken 6. Gedrag van aanvallers 7. Security operations en incident management 8. Forensics
3.	Veiligheid van systemen	9. Cryptografie 10. Operating systems en virtualisation security 11. Distributed systems security 12. Formal methods for security 13. Authentification, authorisation & accountability
4.	Veiligheid van software en platforms	14. Software security 15. Web & mobile security 16. Secure software cycle
5.	Veiligheid van infrastructuur	17. Applied cryptography 18. Network Security 19. Hardware Security 20. Cyber-Physical Systems Security 21. Physical Layer & Telecommunications Security

3.2 Lessen uit eerdere cybercrises

De afgelopen jaren is er zowel in Nederland als internationaal onderzoek gedaan naar diverse cyberincidenten die zich voordeden. Zo trekt Backman (2020) op grond van onderzoek naar twee cybercrises[4] een aantal conclusies met betrekking tot crisis management vereisten. Ze stelt dat als gevolg van de (verwachte) lange duur van cybercrises een beroep gedaan zal worden op de beschikbare technische capaciteit van een organisatie. De respons is daarmee sterk afhankelijk van het vermogen van organisaties om incidentbestrijders met de juiste expertise te mobiliseren, bijvoorbeeld uit de private sector of de cybersecuritygemeenschap (vergelijk IFV, 2021b). Daarnaast geeft ze aan dat plannen en een heldere taak en verantwoordelijkheden in de respons belangrijk zijn. Minstens zo belangrijk echter is volgens Backman het vermogen tot creatief denken, improvisatie en pragmatisme. Dergelijke kennis en vaardigheden zijn van belang vanwege het onvoorspelbare karakter en de vereiste samenwerking tussen partijen die niet eerder met elkaar optrokken.

Ook bruggenbouwers en liaisons moeten volgens Backman onderdeel van de crisisorganisatie uitmaken, doordat cybercrises nooit alleen een ICT-probleem zijn. Dit sluit aan bij de observaties over grensoverschrijdende verbindingen tussen verschillende kennisdisciplines uit hierboven beschreven Cyber Security Body of Knowledge. De liaisons kunnen bijvoorbeeld bijdragen aan het vertalen van technische begrippen en oplossingen naar een breder publiek en als verbindende schakel tussen ICT-experts en de reguliere crisisorganisatie dienen. Communicatie en het geven van accuraat advies aan belanghebbenden wordt gezien als een onontbeerlijke aspect van effectief crisismanagement.

[4] Een ransomware-aanval in Estland in 2007 en een DDOS aanval in het VK in 2017.

Ook uit een beschouwing van diverse cyberincidenten in Nederland (de cyberaanval op de Rotterdamse haven, op Universiteit Maastricht en op de gemeente Lochem, de KPN-storing, en de kwetsbaarheid in de Citrix-software) blijkt, dat veiligheidsregio's momenteel niet beschikken over alle inhoudelijke kennis en kunde die nodig zijn om een cyberverstoring op te lossen (IFV, 2020). Cyberverstoringen als gijzelsoftware vragen specialistische cybersecurityexpertise, onder meer voor het doen van forensisch onderzoek, incidentrespons en het vormgeven van de hersteloperatie (IFV, 2021b). Onderzoekers komen tot de conclusie dat dergelijke kennis en kunde het beste geleverd kunnen worden door partijen als het NCSC, VR-ISAC / CERT en/of branchebrede contracten met specialistische IT-dienstverleners.

Veiligheidsregio's zullen dergelijke expertise een plek moeten geven in de crisisorganisatie, zo blijkt uit bovenstaande onderzoeken. In sommige gevallen is dit al gedaan. Zo heeft Veiligheidsregio Noord- en Oost-Gelderland naar aanleiding van een aanval met een gijzelsoftware op de eigen organisatie in 2020, bijvoorbeeld een crisisorganisatie opgericht, bestaande uit een operationeel team (OT) met vier thematische actiecentra, waaronder forensisch onderzoek en opbouw en herstel (IFV, 2021b). Zo'n model, als het ware een 'OT-Cyber', kan ook voor andere regio's bruikbaar zijn.

Bevorderen cyberkennis-/kunde crisisfunctionarissen
(bron: Werkgroep Digitale ontwrichting en cyber, 9 december 2021)

Vanuit de werkgroep werden de volgende activiteiten genoemd om cyberkennis en -kunde van crisisfunctionarissen te vergroten:

> Oefenen en trainen d.m.v. e-learnings, voorlichtingen, en/ of serious games (regelmatig, laagdrempelig), waarin ook de bestuurlijke kant van een cyberincident wordt beschouwd.
> Kennisdeling uit evaluaties van cyberincidenten in podcasts of sessies.
> Interne dialoog tussen disciplines bevorderen.

3.3 De ISIDOOR-3 oefening

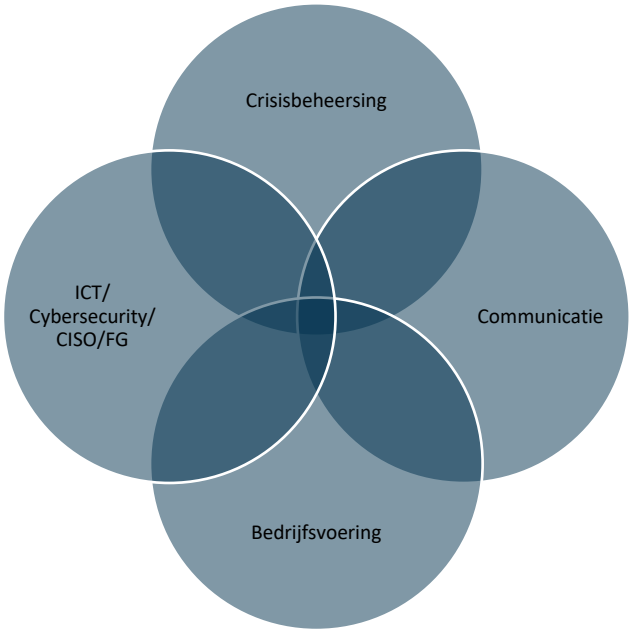
In 2021 vond een grootschalige landelijke cyberoefening plaats, waaraan ook het VR-ISAC, het LOCC en het Operationeel Team (OT) van drie veiligheidsregio's deelnamen.[5] Het IFV heeft in het kader van deze oefening onderzoek gedaan naar het optreden van de deelnemende veiligheidsregio's (IFV, 2021a). Enkele inzichten uit de evaluatie van de oefening in relatie tot cyberkennis en -kunde zijn:

> Crisisfunctionarissen (zoals informatiemanagers, operationeel leiders en communicatie-adviseurs) hebben weinig ervaring met cyberverstoringen. Cyberverstoringen zijn voor crisisfunctionarissen daarmee een betrekkelijk nieuw onderwerp.
> Het gebrek aan ervaring kan bijdragen aan gevoelens van handelingsonbekwaamheid onder crisisfunctionarissen. Door een deelnemer aan de oefening werd dit treffend verwoord met de uitspraak: "We moesten het spel spelen, zonder de regels te kennen".
> Veiligheidsregio's hebben beschikbare kennis voor cybergevolgbestrijding vastgelegd in hulpmiddelen zoals een multidisciplinaire scenariokaart Cyber. Het betreft kennis over opschalings- en alarmeringsprocedures, actoren en netwerkpartners. Het uitwerken van plannen is een manier om meer gevoel en grip op de materie te krijgen. Niettemin lijkt

[5] Voor uitleg over ISIDOOR 2021, zie: https://www.ncsc.nl/onderwerpen/isidoor2021

deze ‘plankennis’ medewerkers slechts een beperkte houvast en gevoel van bekwaamheid te bieden.

> Inzicht dat de wereld van crisisbeheersing en die van cybersecurity aparte kennisdisciplines zijn, maar elkaar bij cyberverstoringen wel nodig hebben voor onder meer beeld- en oordeelsvorming en besluitvorming over maatregelen.



Figuur 3.2 Cyberverstoringen: intern verbinden van werelden

Aanvullend bleek het voor deelnemende teams tijdens de oefening lastig om beeld, laat staan een goed begrip, te krijgen van de bredere cyberresponsoperatie. Dergelijk gedeeld begrip of situationeel bewustzijn is voor specialistische teams nodig om hun eigen plek binnen de bredere responsorganisatie beter te kunnen plaatsen en te beseffen hoe hun team bijdraagt aan het grotere geheel (zie ook: McChrystal e.a., 2019). Dit sluit aan bij de opmerkingen over kennis en kunde in paragraaf 1.2, waarbij het niet alleen gaat over ‘weten en kennen’, maar ook over ‘begrijpen’; begrijpen van de context waarin je als team of specialist opereert en begrijpen van het grotere geheel waarvan je deel uitmaakt.

Het COT (2021a) benoemt dat beperkte kennis over en inzicht in cybersecurityaspecten bij crisisfunctionarissen het inschatten van de impact en maatregelen tijdens de ISIDOOR-3 oefening bemoeilijkten. Daarbij komt tevens de uitdaging van ‘taal’: specifieke technische materie die inzichtelijk moet worden gemaakt. De welbekende kloof tussen ICT en crisis wordt ook onder vitale partners herkend. Eén van de oplossingen is volgens het COT het organiseren van een ‘linking pin’ (bijvoorbeeld een verbindingsofficier) tussen het IT-team en het crisisteam. De verbindingsofficier vormt de schakel tussen de IT-operatie en de bredere crisisbeheersing. De verbindingsofficier beschikt over basiskennis van IT en weet zijn IT-specialisten de juiste vragen te stellen, maar weet ook hoe de crisisorganisatie van het bedrijf functioneert.

De verbindingsofficier onderhoudt verder de contacten met de leiders van operationele processen en teams. Daarbij kunnen op het gebied van cybersecurity diverse kennisgebieden worden onderscheiden, waaronder:

> analyse van cyberdreigingen
> monitoring en detectie
> forensisch onderzoek
> eigen IT-systemen (hardware, software)
> vitale processen.

Kennisoverdracht tussen IT security en bestuur (bron: OZON, 2018; COT, 2021b)
Voortkomend uit oefeningen en daadwerkelijke cyberincidenten in het hoger onderwijs worden de volgende aanbevelingen geformuleerd voor het overbruggen van de kloof tussen IT security en crisisbeheersing (OZON, 2018; COT, 2021b):

1. Zorg dat de technische security teams beter in staat zijn hun kennis over te dragen aan het tactische en strategische niveau.
2. Biedt het tactisch en strategisch niveau basis-cybersecuritykennis om de communicatie en begrip richting operationeel niveau te verbeteren
3. Organiseer voldoende technische security kennis en vaardigheden op operationeel niveau voor de respons op cybercrises

Hierbij kan de CISO, zo schrijft het COT, een belangrijke rol vervullen in het vertalen van technische informatie en als schakel tussen de verschillende teams, zoals IT security, communicatie en bestuur. Het COT (2021b, 26): “Zo heeft de CISO een overzichtelijke uitleg van de cyber kill chain gegeven en verteld hoe de aanval verloopt. Dit overzicht is gewenst om de brug te slaan tussen de daadwerkelijke technische informatie en gevolgen en consequenties voor de bestuurlijke wereld” . In de evaluatie wordt tevens het belang van scenariodenken benoemd; een methode waar inhoudelijke expertise en kunde samenkomen.

Tot een bepaalde graad kunnen vitale organisaties cyberincidenten zelf verhelpen, maar bij grote verstoringen is specifieke cybersecurityexpertise nodig. Hiervoor wordt gebruikgemaakt van ‘retainer contracten’: cybersecurityexperts op wie een beroep kan worden gedaan in geval van nood. Bij grote verstoringen bestaat dus de mogelijkheid om bedrijven als Fox-IT of het NSCS te bellen voor extra hulp. Over het algemeen wordt daarnaast ook in de koude fase intensief samengewerkt met het NSCS voor het delen van kwetsbaarheden en cyberdreigingen.

Het beter verbinden van beide werelden en het vergroten van wederzijds begrip vraagt, zo schatten wij in, een inspanning van beide kanten. Er is behoefte aan crisisfunctionarissen die zich actief verdiepen in cyber én ICT-experts die begrip opdoen voor de werkwijzen van crisismanagement.

4 Bevindingen

Dit hoofdstuk geeft antwoorden op de onderzoeksvragen. Het gaat in op beschikbare en ontbrekende kennis en kunde en op mogelijkheden om die kennis en kunde voor het bestrijden van cyberverstoringen te mobiliseren.

4.1 Overkoepelende bevindingen

1. Uit het onderzoek blijkt dat de kennis en kunde voor de bestrijding van cyberverstoringen in veiligheidsregio's beperkt aanwezig zijn. Voor veiligheidsregio's is het lastig meer ervaring en expertise op te bouwen in dit nieuwe crisisdomein, doordat het aantal cyberverstoringen waarbij de inzet van regio's nodig is, (tot op heden) beperkt is. De vraag welke kennis en kunde nodig zijn, is nog niet zo eenvoudig te beantwoorden, temeer daar cybercrisismanagement een betrekkelijk jonge discipline is. De vraag welke expertise nodig is, hangt bovendien samen met de omvang, ernst en complexiteit van de verstoring die zich voordoet.[6] De in dit onderzoek geïnventariseerde cyberkennis en -kunde vormen een startpunt voor nader onderzoek, dialoog en opbouw van een 'body of knowledge'.
2. Voor interne cyberverstoringen als gijzelsoftware hebben veiligheidsregio's specialistische cybersecurityexpertise nodig, onder meer voor forensisch onderzoek, incidentrespons en het vormgeven van de hersteloperatie. Veiligheidsregio's hoeven hier niet zelf over te beschikken; zij zijn tenslotte géén cyberspecialisten. Meer specialistische kennis en kunde kan geleverd worden door partijen als het NCSC, VR-ISAC / CERT en/of branchebrede contracten met specialistische IT-dienstverleners. Op het gebied van cybersecurity en -respons is inmiddels vanuit het Verenigd Koninkrijk een 'body of knowledge' cybersecurity beschikbaar. Voor veiligheidsregio's kan dit document een middel zijn om de eigen kennispositie op het gebied van cybersecurity te inventariseren: welke expertise hebben regio's zelf in huis, welke kennis hebben ze nodig, en welke expertise kunnen andere partijen zoals universiteiten, hogescholen of bedrijven leveren?
3. Veiligheidsregio's hebben beschikbare kennis voor cybergevolgbestrijding vastgelegd in hulpmiddelen zoals een multidisciplinaire scenariokaart cyber. Ook wordt gewerkt aan het Landelijk Crisisplan Digitaal. Dit plan bevat kennis over opschalings- en alarmeringsprocedures, actoren en netwerkpartners. Dergelijke kennis over actoren en hun taken en verantwoordelijkheden is noodzakelijk. Niettemin lijkt deze feitelijke kennis crisisfunctionarissen slechts een beperkte houvast en gevoel van bekwaamheid te bieden; het gaat ook om ervaring en begrip van de dynamiek en dilemma's die spelen bij een cybercrisis. Zoals we in paragraaf 1.2 hebben opgemerkt, zullen beroepsbeoefenaren over méér moeten beschikken dan feitelijke kennis; het gaat juist ook om bredere begripsvorming ('Verstehen') en het *toepassen* van kennis in verschillende praktijksituaties. In dat licht is er nood aan het opbouwen van een steviger ervaringsniveau, bijvoorbeeld door oefenen én het versterken van de samenwerking en een wederzijds begrip tussen de

[6] Veiligheidsregio's kunnen zelf getroffen worden door een cyberverstoring, als crisisbestrijder een rol spelen bij een verstoring bij vitale en maatschappelijke organisaties of een combinatie van beide.

kennisdisciplines ICT / cybersecurity en crisisbeheersing. Die disciplines hebben elkaar nodig voor een goed begrip van de situatie, voor beeld- en oordeelsvorming en besluitvorming over de benodigde maatregelen.

4.2 Beschikbare kennis en kunde in veiligheidsregio's

> Het merendeel van de veiligheidsregio's is van mening dat de regio zelf verantwoordelijk is voor het inventariseren van interne dreigingen. Slechts de helft heeft hiervoor echter de nodige kennis en kunde. De inventarisatie van externe dreigingen, bijvoorbeeld voor vitale infrastructuur, is volgens de meeste regio's voornamelijk een zaak van externe partners.
> Veiligheidsregio's zijn nauwelijks in staat om zelf de oorzaak en duur van interne en externe incidenten in te schatten. Wel vinden ze het belangrijk om zelf de nodige kennis en kunde te hebben om de effecten en impact van interne en externe cyberincidenten in te kunnen schatten.[7] Met name wat betreft interne (maar in geringere mate ook externe) incidenten zijn de nodige kennis en kunde beperkt. Hier bestaat dus ruimte voor verbetering.
> Binnen het management van veiligheidsregio's bestaan over het algemeen bewustzijn en belangstelling voor cyber, maar duidelijk meer voor externe dan voor interne dreigingen. Bij operationele functionarissen is daarentegen gemiddeld juist iets meer aandacht voor interne dan voor externe cyberdreigingen.
> Veiligheidsregio's hebben duidelijk meer kennis en kunde om de effecten van externe dan van interne incidenten te beperken. Het merendeel vindt dan ook dat de regio (mede)verantwoordelijk is voor *externe* cybergevolgbestrijding. Over wat de juiste plek is voor kennis en kunde voor de gevolgbestrijding van *interne* verstoringen lopen de meningen echter uiteen.
> Hoewel het bewustzijn ten aanzien van digitale dreigingen redelijk hoog lijkt te zijn (dit geldt in ieder geval voor het bestuurlijke niveau), lijken er weinig financiële middelen, tijd en capaciteit beschikbaar te zijn voor de voorbereiding op zowel interne als externe incidenten binnen het cyberdomein.
> Theoretisch hebben veiligheidsregio's voldoende zicht op externe partijen die ze kunnen benaderen bij een intern of extern cyberincident. Wel bestaat er nog onduidelijkheid over de verantwoordelijkheden van zowel veiligheidsregio's als partners.

4.3 Benodigde kennis en kunde

> Voor de voorbereiding op interne cyberincidenten ontbreekt het vooral aan bewustzijn, tijd, capaciteit en financiële middelen in de veiligheidsregio's. Zo blijkt dat er niet voldoende tijd wordt gereserveerd binnen de regio's om voorbereidingen te treffen voor digitale verstoringen en zijn er niet voldoende personeel en financiële middelen beschikbaar. Ook wordt het thema cyber nog weleens als 'ingewikkeld' ervaren. ICT-medewerkers en CISO's zouden volgens de regio's voornamelijk verantwoordelijk moeten zijn voor het borgen van de nodige cyberkennis en -kunde. Respondenten geven aan dat er binnen de organisatie meer sprake zou moeten zijn van

[7] Bij externe cyberincidenten zijn regio's altijd afhankelijk van derden. Veiligheidsregio's kunnen de impact van een cyberincident op de vitale processen van maatschappelijke partners niet inschatten. Daar hebben zij altijd de betrokken partij voor nodig.

bewustwording, auditing en lerend vermogen met betrekking tot cyberincidenten. Het blijkt voor regio's hierbij een uitdaging om ingewikkelde onderwerpen rondom cyber toegankelijk te maken voor functionarissen.

> Wat betreft kennis en kunde over interne cyberincidenten zijn volgens de respondenten met name ICT-medewerkers belangrijke spelers.
> Voor de gevolgbestrijding van externe cyberincidenten zou kennis volgens de respondenten binnen de eigen organisatie bij medewerkers crisisbeheersing moeten liggen, zo geeft bijna de helft van de respondenten aan. Daarnaast geeft ongeveer een kwart van de respondenten aan de kennis binnen de organisatie (ook) bij een CISO te willen beleggen.
> Voor het verbeteren van externe cybergevolgbestrijding is er vooral behoefte aan een goed netwerk met partners. Hierbij gaat de voorkeur van regio's uit naar NCSC, private kennis- en adviesbureaus en publieke kennisinstellingen (dit geldt overigens ook voor eventuele ondersteuning bij interne cyberincidenten). Ook risicobewustzijn en cyberkennis verdienen volgens de regio's aandacht. Binnen de regio's lijken crisisfunctionarissen nog de meest geschikte personen om kennis en kunde voor externe cybergevolgbestrijding te borgen.
> Veiligheidsregio's zouden zichzelf de vraag moeten stellen welke ervaring en deskundigheid zij al in huis hebben. Denk hierbij aan functionarissen en disciplines zoals een Functionaris Gegevensbescherming (FG), een CISO en ICT. Vervolgens zouden zij met deze functionarissen in gesprek moeten gaan over de vraag welke bijdrage zij kunnen leveren aan de incident- en crisismanagementrespons.

4.4 Cyberkennis en -kunde voor gevolgbestrijding

De in dit onderzoek geïnventariseerde kennis en kunde voor cybergevolgbestrijding hebben we als wijze van samenvatting weergegeven in tabel 4.2 op de volgende pagina.

Tabel 4.2 Cyberkennis en -kunde voor gevolgbestrijding

Cyberkennis en -kunde voor gevolgbestrijding	
Cyberkennis	> Nationaal Crisisplan Digitaal / actoren, taken en verantwoordelijkheden / Netwerk van crisisorganisaties bij partners kennen en cyberspecifieke teams (o.a. IBD, Zorg-CERT, NCSC) > Handreiking Cybergevolgbestrijding (diagnose, methoden, maatregelen) > Scenariokaarten Cyber > Rollen veiligheidsregio's: risicoadviseur, netwerkregisseur, bijstandsverlener, probleemeigenaar en gevolgbestrijder > Rol en taken VR-ISAC > Bewustzijn van eigen rol en wat daar wel / niet bij hoort > Bestuurlijke uitgangspunten en dilemma's bij cyber
Cyberkunde (vaardigheden en houding)	> Creatief denken > Improvisatievermogen > Pragmatisme > Bescheidenheid: niet alles zelf willen doen > Netwerkvaardigheden

- Open, nieuwsgierige houding / vragen stellen
- Ervaring (oefenervaring, praktijkervaring)
- Scenariodenken, duiden en monitoren
- Vertaalvermogen / advieskracht specialisten en bestuur / crisisbeheersing
- Vertaalvermogen cyber / ICT naar (maatschappelijke) impact
- Bruggenbouwers / liaisons /schakelvermogen operatie-tactisch-strategisch

5 Advies over mobiliseren van cyberkennis en -kunde

5.1 Versterken van kennis en kunde binnen de eigen veiligheidsregio

Uit diverse studies blijkt dat meerdere kennisdisciplines (ICT, cybersecurityexpertise, crisisbeheersing, bedrijfsvoering) nodig zijn voor de respons op cyberincidenten én dat die disciplines onderling te weinig verbonden zijn. Hieronder geven we aangrijpingspunten om de verschillende disciplines beter met elkaar te verbinden.

> Verhogen van het kennispeil over cyber onder crisisfunctionarissen zoals operationeel leiders en communicatieadviseurs en onder bedrijfsvoering is nodig, door bijvoorbeeld bijscholing, het uitwisselen van ervaringen met collega's, kennisnemen en doorleven van planvorming en oefenen. Dit is relevant voor de bestrijding van interne en externe cyberincidenten. Bijscholing zou in elk geval de onderwerpen uit tabel 4.2 betreffen, waaronder van de partners die over kennis beschikken bij een cybercrisis.

> Verhogen van het kennispeil van crisisbeheersing onder ICT-functionarissen door bijvoorbeeld bijscholing, meedoen met crisisoefeningen, kennisnemen en doorleven van planvorming. Dat is relevant voor de bestrijding van interne cyberincidenten.

> Het is nodig om binnen de organisatie te investeren in bruggenbouwers of liaisons die verschillende kennisdisciplines met elkaar kunnen verbinden. Denk aan een tactisch-strategisch ingestelde 'OvD-Cyber' of adviseur Cyber. Zie voor de benodigde kennis en kunde van zo'n functionaris tabel 4.2.

> Gezamenlijke scenariobijeenkomsten waarin verschillende disciplines in gesprek gaan over de bijdrage die zij kunnen leveren aan de incidentrespons zijn onontbeerlijk. Wat kunnen de disciplines tijdens cyberverstoringen van elkaar verwachten? Wat kunnen zij wel en wat ook niet leveren?

5.2 Collectief versterken van kennis en kunde

Veiligheidsregio's zijn niet gespecialiseerd in cybersecurity: het zijn veiligheidsregio's en geen 'cybersecurityregio's'. Bij verstoringen waarbij regio's zelf slachtoffer zijn, kan er nood zijn aan specialistische cybersecurityexpertise. Collectieve inkoop is voor veiligheidsregio's één van de mogelijkheden om te beschikken over gegarandeerde kennis en kunde bij cyberverstoringen. Niettemin blijft het noodzakelijk te investeren in de eigen cyberweerbaarheid, onder meer op het gebied van monitoring en incidentrespons én door het bekwamen van crisisfunctionarissen middels het aanbieden van een opleiding of cybermodule.

Bronnen

Backman, S. (2020). Conceptualizing cyber crises. *Journal of Contingencies and Crisis Management, 29*(31), 429-439. Ontleend aan https://onlinelibrary.wiley.com/doi/full/10.1111/1468-5973.12347.

COT (2021a), *Leerpunten cyberoefening ISIDOOR 2021. Snelheid maken & impact beperken*, Rotterdam: COT Instituut voor Veiligheids- en Crisismanagement.

COT (2021b), *'Aanval afgeslagen'. Leerevaluatie cyberaanval Hogeschool van Amsterdam en Universiteit van Amsterdam*, Rotterdam: COT Instituut voor Veiligheids- en Crisismanagement.

Cyber Security Body of Knowledge (2019), *Introduction to CyBOK Knowledge Area*, Crown Copyright, The National Cyber Security Centre.

Evaluatiecommissie Wet veiligheidsregio's. (2020). *Evaluatie Wet veiligheidsregio's, naar toekomstbestendige crisisbeheersing en brandweerzorg.*

Instituut Fysieke Veiligheid (2019). *Whitepaper digitale ontwrichting en cyber.* Arnhem: IFV.

Instituut Fysieke Veiligheid (2020a). *Cyberrisico's en veiligheidsregio's. Hoe beoordelen veiligheidsregio's cyberrisico's?* Arnhem: IFV.

Instituut Fysieke Veiligheid (2020b). *Cybergevolgbestrijding: lessen uit cyberverstoringen in Nederland.* Arnhem: IFV.

Instituut Fysieke Veiligheid (2020c). *Versterken van veerkracht. Naar een gezamenlijke aanpak van ongekende crises.* Arnhem: IFV.

Instituut Fysieke Veiligheid (2021a), *Evaluatie veiligheidsregio's ISIDOOR-3*, Arnhem: IFV.

Instituut Fysieke Veiligheid (2021b), *Gijzelsoftware Veiligheidsregio Noord- en Oost-Gelderland. Evaluatie van de crisisrespons*, Arnhem: IFV.

McChrystal, S., Collins, T., Silvermand, D., Fussell, C. (2019), *Team of teams. New rules of Engagement for a Complex World*, Penguin Random House UK.

NCTV. (2020a). *Cybersecuritybeeld Nederland.* Den Haag: NCTV.

NCTV. (2020b). *Nationaal Crisisplan Digitaal.* Den Haag: NCTV.

Romiszowski, A. J. (1981). *Designing instructional systems*. New York, NY: Nichols.

Weggeman, M (2007). *Leidinggeven aan professionals? Niet doen!. Over kenniswerkers, vakmanschap en innovatie*. Schiedam: Scriptum